REMARKS

Claims 1-21 remain in the application without further amendment.

In the final Office Action mailed February 18, 2010, the Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) as unpatentable over Mills (U.S. Patent No. 6,311,204) and further in view of Ducharme (U.S. Patent No. 7,165,180).

In remarks accompanying the rejection, the Examiner states:

> Although Mills discloses receiving common key in encrypted form by broadcast signal (e.g. col. 11, lines 9-50), Mills may not explicitly disclose that the common key is stored in decrypted form in an integrated circuit, whereby the circuit is arranged such that the only route to placing a common key in the common key store is to receive in encrypted from [sic] for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key, neither may not explicitly disclose a secret key store is located in the integrated circuit or having common key store and secret key store in a monolithic device which configured to store common key and secret key.

Applicants also note that the claimed secret key store is also not present in Mills. Rather, Mills relies upon a smart card (80), which is in apposite to the intent and purposes of the present claimed embodiments. In other words, as argued in the last Amendment, which applicants adopt herein by reference in their entirety, the present embodiments are designed, in part, to provide increased security by eliminating the interface between a secret key store and the decryption unit. Hence, in the present claimed embodiments, the secret key store is part of the monolithic integrated circuit.

To provide the foregoing missing features, the Examiner relies upon the secondary reference, Ducharme. More particularly, Ducharme describes the use of a control key store or encryption key register (130). The Examiner asserts that this "teaches the concept of having a common key store in an integrated circuit and/or in a monolithic device" (see page 5, lines 6-7 of the remarks accompanying the final Office Action of February 18, 2010).

Applicants vigorously and respectfully disagree. The key register (130) of Ducharme is more akin to the smart card (80) of Mills because Ducharme teaches that the key register (130) is used to store an encryption key. See column 3, lines 22-26 in which Ducharme states:

> In at least one embodiment, an encryption key stored in key register **130** is provided to encryption engine **120**. Encryption engine **120** can then use part or all of the encryption key to perform an encryption/decryption function on data.

Ducharme further states at column 4, lines 26-32:

> Accordingly, the contents (i.e. the encryption key) of key register **130** of monolithic semiconductor device **100**, in at least one embodiment, are inaccessible, i.e. unobservable, to any device external to monolithic semiconductor device **100**. Similarly, in one embodiment, the contents of key register **130** are observable only by encryption engine **120**.

At page 4, second paragraph of the remarks accompanying the final Office Action;, the Examiner quotes from Mills, in which the "smart card stores a secret key for the processing system 10 and uses the secret key to decrypt an encrypted service key and thereby authenticate the EMM information." Clearly the key register 130 in Ducharme is more equivalent to the smart card (80) of Mills.

Thus, the key register (130) of Ducharme is not a common key store for a decrypted common key. On page 5 of the remarks, near the end of the second paragraph the Examiner states:

> …and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key, neither may not explicitly disclose a secret key store is located in the integrated circuit or having common key store and secret key store in a monolithic device which configured to store common key and secret key…

Applicants are unclear what the Examiner is arguing in this portion of the Remarks. It does appear to the applicants, however, that if the Examiner is arguing that the key register (130) of Ducharme replaces the smart card (80) of Mills. This, however, is not teaching or suggesting a decrypted a common key store. The element clearly missing from the combination of Ducharme and Mills is the decrypted common key store that stores a plurality of decrypted common keys.

In other words, neither Ducharme nor Mills, taken alone or in any combination thereof, teach or suggest a common key store for storing a decrypted common key or a plurality of decrypted common keys (see dependent claim 7, which depends from claim 1 of the present claims, which is directed to the common key store storing "multiple common keys").

At paragraph 10 on page 7 of the remarks in the Office Action, the Examiner asserts that Ducharme teaches a common key store storing multiple common keys. For example, the Examiner references column 2, lines 18-50 of Ducharme. However, at line 26, Ducharme refers to storing "encryption keys" not decrypted common keys. Also, at column 2, lines 29-30, Ducharme again refers to an "encryption key register to store one or more encryption keys" (emphasis added). With respect to the Examiner's reliance on column 7, lines 58-67, there Ducharme is describing the storage of a private key in the key register (130) for subsequent use by the encryption engine and the separate storage of a public key (602) that is stored locally in a memory or register internal to the encryption engine (120) or in memory used by one or more elements of the semiconductor device, such as memory (140). Nowhere does Ducharme teach or suggest a separate decrypted common key store that stores multiple decrypted common keys in a single memory in which the encrypted common keys are decrypted on the monolithic circuit using the secret key stored on the same circuit.

At best, Ducharme describes the encryption engine having access to a plurality of public keys corresponding to different sized portions of the 128-bit private encryption key. As stated at column 4, lines 2-11:

> For example, the first forty bits of the private key in key register 130 can be used in conjunction with a corresponding public key to provide minimum security, the first 64 bits of the private key can be used in conjunction with a corresponding public key to provide moderate security, and the full 128 bits can be used in conjunction with a different corresponding public key to provide a high level of security. Alternatively, key register 130 can include a plurality of encryption keys with the same or different bit lengths.

The Examiner makes an effort to rebut applicants' arguments in the last amendment by relying, in part, on the common knowledge in the art. In other words, where the references are silent, the Examiner asserts the differences between the combination of the references and the claimed features are "well known in the art for a long time," such as the storage of multiple decrypted common keys in a register. In addition, the Examiner asserts that because Mills teaches the service keys changing at a low rate (days or months), that temporary storage in the receiver is implied since there is “no need for [sic] keep sending the same service keys over and over again.”

It is clear that applicants’ combination recited in claims 1-21 is new over the art of record. Applicants respectfully submit the Examiner has not met his burden of providing a *prima facie* case of obviousness by relying on a combination of Mills, Ducharme, and the asserted common knowledge in the art. Even if one were to combine all three, they would fail to meet the limitations of claims 1-21 because there is no teaching or suggestion in either Mills or Ducharme to modify them in accordance with what the Examiner asserts is common knowledge in the art.

For example, Mills is directed to a processing system with a register-based process sharing scheme. Mills does not recognize the potential security breach that can occur with the use of a smart card (80).

While Ducharme attempts to overcome this problem by utilizing a private key or encryption key stored in the key register (130) on a monolithic circuit, Ducharme does not teach or suggest the additional feature recited in the claims of receiving, decrypting, and storing common keys in a common key store formed internally on the monolithic integrated circuit. This methodology and corresponding circuit eludes Ducharme, although Ducharme issued in 2007, which was six years after Mills.

Only until Applicants submitted their approach in the present disclosure was it recognized that additional security can be provided through the method and circuit as recited in claims 1-21 of the present application. For the Examiner to supply the missing recited elements by relying on common knowledge in the art is insufficient to meet his obligation to provide a *prima facie* basis for an obviousness rejection. Moreover, it appears to be the impermissible use of hindsight.

For example, nowhere does Ducharme recognize that reception of a public key in combination with a private key for asymmetrical encryption methods is less secure than utilizing both encrypted common key and stored secret key for ultimately decrypting control words as in the present disclosure. At column 3, lines 46-52, Ducharme states:

> Alternatively, in at least one embodiment, the encryption key stored in key register **130** includes an asymmetrical key used by asymmetrical encryption methods such as the RSA. In asymmetrical encryption methods, one key is used to encrypt data (the public key of the recipient of the encrypted data) and one key is used to decrypt encrypted data (the private key of the recipient). For example, as discussed in greater detail with reference to FIG. 7, encryption engine **120** can include an asymmetrical encryption engine and additional component **150** can include a symmetrical encryption engine. In this case, encryption engine **120** be used to decrypt an encrypted control word, and the control word can then be provided to the symmetrical encryption engine (additional component **150**) to decrypt data encrypted by another device or system using the control word.

As described here, Ducharme utilizes a staged decryption of an encrypted control word that is then used to decrypt encrypted data, which is only half of what applicants are describing and claiming in the present application.

In view of the foregoing, applicants respectfully submit that claims 1-21 are non-obvious over the combination of Mills, Ducharme, and "common knowledge in the art."

In the event the Examiner still disagrees or finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jl
701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1602152_1.DOC